Criptografia do Mundo Real

David Wong

Conteúdo

Prefácio

Como você pegou este livro, pode estar se perguntando: por que mais um livro sobre criptografia? Ou até mesmo, por que eu deveria ler este livro? Para responder a isso, você precisa entender quando tudo começou.

Um livro, anos em formação

Hoje em dia, se você quer aprender sobre quase qualquer coisa, você procura no Google, ou Bing, ou Baidu — você entendeu. No entanto, para criptografia, e dependendo do que você está procurando, os recursos podem ser bastante escassos. Isso foi algo que enfrentei há muito tempo e que tem sido uma fonte contínua de frustração desde então.

Na época em que eu estava na escola, tive que implementar um ataque de análise de potência diferencial para uma aula. Esse ataque foi um avanço na criptoanálise naquela época, sendo o primeiro ataque de canal lateral publicado. Um ataque de análise de potência diferencial é algo mágico: ao medir o consumo de energia de um dispositivo enquanto ele criptografa ou descriptografa algo, você consegue extrair seus segredos. Eu percebi que artigos excelentes podiam transmitir grandes ideias, mas com pouco esforço em clareza e inteligibilidade. Lembro de bater a cabeça na parede tentando entender o que o autor queria dizer. Pior, eu não conseguia encontrar bons recursos online que explicassem o artigo. Então bati a cabeça mais um pouco e finalmente entendi. E então pensei, talvez eu pudesse ajudar outros como eu que teriam que passar por essa provação.

Motivado, desenhei alguns diagramas, os animei e gravei a mim mesmo explicando-os. Esse foi meu primeiro vídeo no YouTube sobre criptografia:
https://www.youtube.com/watch?v=gbqNCgVcXsM

Anos depois, ainda recebo elogios de pessoas aleatórias na internet. Ontem mesmo, enquanto escrevo este prefácio, alguém comentou: "Obrigado, realmente uma explicação ótima que provavelmente me salvou horas tentando entender aquele artigo."

Que recompensa! Esse pequeno passo em me aventurar no outro lado da paisagem educacional foi suficiente para me fazer querer fazer mais. Comecei a gravar mais desses vídeos e, em seguida, iniciei um blog para escrever sobre criptografia. Você pode conferir aqui: https://cryptologie.net

Antes de começar este livro, eu já havia acumulado quase 500 artigos explicando os muitos conceitos além desta introdução. Tudo isso era apenas prática. No fundo da minha mente, a ideia de escrever um livro vinha amadurecendo anos antes de a Manning Publications entrar em contato comigo com uma proposta.

O currículo do criptógrafo do mundo real

Terminei minha graduação em matemática teórica e não sabia o que fazer a seguir. Eu também programava desde sempre e queria reconciliar as duas coisas. Naturalmente, fiquei curioso sobre criptografia, que parecia reunir o melhor dos dois mundos, e comecei a ler os livros disponíveis. Rapidamente descobri minha vocação.

Mas havia algumas coisas irritantes: especialmente as introduções longas que começavam com história; eu estava interessado apenas nos aspectos técnicos e sempre fui assim. Jurei para mim mesmo: se algum dia eu escrevesse um livro sobre criptografia, não escreveria uma única linha sobre cifras de Vigenère, cifras de César e outros vestígios da história. E assim, depois de obter um mestrado em criptografia na Universidade de Bordeaux, achei que estava pronto para o mundo real. Mal sabia eu...

Acreditei que meu diploma era suficiente, mas minha educação carecia muito dos protocolos do mundo real que eu estava prestes a analisar. Passei muito tempo aprendendo sobre a matemática das curvas elípticas, mas nada sobre como elas eram usadas em algoritmos criptográficos. Aprendi sobre LFSRs, ElGamal, DES e uma série de outras primitivas criptográficas que nunca mais veria novamente.

Quando comecei a trabalhar na indústria, na Matasano, que depois se tornou NCC Group, meu primeiro trabalho foi auditar o OpenSSL, a implementação SSL/TLS mais popular — o código que basicamente criptografava toda a internet. Oh, como aquilo doía minha cabeça. Lembro de voltar para casa todo dia com uma forte dor de cabeça. Que bagunça de biblioteca e protocolo! Eu não sabia na época que, anos depois, me tornaria coautor do TLS 1.3, a versão mais recente do protocolo.

Mas, naquele ponto, já estava pensando: "É isso que eu deveria ter aprendido na faculdade. Este conhecimento que estou adquirindo agora é o que teria sido útil para me preparar para o mundo real!" Afinal, eu era agora um especialista em segurança especializado em criptografia. Eu revisava aplicações criptográficas do mundo real. Eu fazia o trabalho que qualquer um desejaria após terminar um curso de criptografia. Eu implementava, verificava, usava e aconselhava quais algoritmos criptográficos usar. É por isso que sou o primeiro leitor do livro que estou escrevendo. Este é o livro que eu teria escrito para meu eu do passado para prepará-lo para o mundo real.

Onde estão a maioria dos erros

Meu trabalho como consultor me levou a auditar muitas aplicações criptográficas do mundo real, como o OpenSSL, o sistema de backup criptografado do Google, a implementação do TLS 1.3 da Cloudflare, o protocolo da autoridade certificadora da Let’s Encrypt, o protocolo sapling da criptomoeda Zcash, o esquema de recriptografia por procuração com limiar da NuCypher, e dezenas de outras aplicações criptográficas do mundo real que, infelizmente, não posso mencionar publicamente.

Logo no início do trabalho, fui encarregado de auditar o protocolo personalizado que uma corporação famosa havia escrito para criptografar suas comunicações. Acontece que ele usava assinaturas em quase tudo, exceto nas chaves efêmeras, o que quebrava completamente o protocolo, já que alguém poderia facilmente substituí-las — um erro básico para qualquer um com alguma experiência com protocolos de transporte seguros, mas algo que foi negligenciado por pessoas que pensavam ter experiência suficiente para criar sua própria criptografia. Lembro de explicar a vulnerabilidade no final do trabalho e de ver uma sala cheia de engenheiros ficar em silêncio por bons 30 segundos.

Essa história se repetiu muitas vezes durante minha carreira. Houve uma vez em que, ao auditar uma criptomoeda para outro cliente, encontrei uma maneira de forjar transações a partir de transações já existentes, devido a uma ambiguidade sobre o que estava sendo assinado. Ao olhar implementações de TLS para outro cliente, encontrei maneiras sutis de quebrar uma implementação de RSA, o que, por sua vez, se transformou em um artigo técnico com um dos inventores do RSA, levando a diversos relatórios de CVEs (Common Vulnerabilities and Exposures) para dúzias de projetos de código aberto. Mais recentemente, ao estudar o novo protocolo de chat Matrix enquanto escrevia este livro, percebi que seu protocolo de autenticação estava quebrado, o que levava à quebra de sua criptografia de ponta a ponta. Há tantos detalhes que, infelizmente, podem ruir quando se utiliza criptografia. Nesse ponto, eu sabia que precisava escrever algo sobre isso. Por isso, meu livro contém muitas dessas anedotas.

Como parte do trabalho, eu revisava bibliotecas e aplicações criptográficas em uma infinidade de linguagens de programação. Descobri bugs (por exemplo, o CVE-2016-3959 na biblioteca padrão do Golang), pesquisei maneiras pelas quais bibliotecas poderiam induzir ao uso incorreto (por exemplo, meu artigo "How to Backdoor Diffie-Hellman"), e aconselhei sobre quais bibliotecas usar. Os desenvolvedores nunca sabiam qual biblioteca usar, e eu sempre achava a resposta complicada.

Acabei por inventar o protocolo Disco (https://discocrypto.com; https://embeddeddisco.com) e escrevi sua biblioteca criptográfica completa em menos de 1.000 linhas de código — e isso, em várias linguagens. Disco se baseava apenas em duas primitivas criptográficas: a permutação do SHA-3 e a Curve25519. Sim, com apenas essas duas coisas implementadas em 1.000 linhas de código, um desenvolvedor poderia realizar qualquer tipo de troca de chaves autenticada, assinaturas, criptografia, MACs, hashing, derivação de chaves e assim por diante. Isso me deu uma perspectiva única sobre o que uma boa biblioteca de criptografia deveria ser.

Quis que meu livro contivesse esses tipos de insights práticos. Assim, naturalmente, os diferentes capítulos contêm exemplos de como aplicar "criptografia" em diferentes linguagens de programação, usando bibliotecas criptográficas bem respeitadas.

A necessidade de um novo livro?

Enquanto eu ministrava uma das minhas sessões anuais de treinamento em criptografia na Black Hat (uma conhecida conferência de segurança), um aluno veio até mim e perguntou se eu poderia recomendar um bom livro ou curso online sobre criptografia. Lembro de ter aconselhado o aluno a ler um livro de Boneh e Shoup e assistir ao curso *Cryptography I* de Boneh no Coursera. (Eu também recomendo ambos os recursos ao final deste livro.)

O aluno me disse: "Ah, eu tentei, mas é muito teórico!" Essa resposta ficou comigo. Discordei a princípio, mas aos poucos percebi que ele estava certo. A maioria dos recursos são bastante pesados em matemática, e a maioria dos desenvolvedores que lidam com criptografia não quer lidar com matemática. O que mais havia para eles?

Os outros dois recursos um tanto respeitados na época eram *Applied Cryptography* e *Cryptography Engineering* (ambos livros de Bruce Schneier). Mas esses livros estavam começando a ficar bastante desatualizados. *Applied Cryptography* dedica quatro capítulos a cifras de bloco, com um capítulo inteiro sobre modos de operação de cifra, mas nenhum sobre criptografia autenticada. O mais recente *Cryptography Engineering* fazia uma única menção à criptografia de curva elíptica em uma nota de rodapé. Por outro lado, muitos dos meus vídeos ou posts de blog estavam se tornando boas referências primárias para alguns conceitos criptográficos. Eu sabia que poderia fazer algo especial.

Gradualmente, muitos dos meus alunos começaram a se interessar por criptomoedas, fazendo cada vez mais perguntas sobre o assunto. Ao mesmo tempo, comecei a auditar mais e mais aplicações de criptomoeda. Mais tarde, fui trabalhar no Facebook liderando a segurança da criptomoeda Libra (agora conhecida como Diem). Criptomoedas eram, na época, um dos campos mais quentes para se trabalhar, misturando uma multiplicidade de primitivas criptográficas extremamente interessantes que até então tinham visto pouco ou nenhum uso no mundo real (provas de conhecimento zero, assinaturas agregadas, criptografia com limiar, computações multipartidárias, protocolos de consenso, acumuladores criptográficos, funções aleatórias verificáveis, funções de atraso verificáveis, ... a lista continua). E ainda assim, nenhum livro de criptografia incluía um capítulo sobre criptomoedas. Eu estava agora em uma posição única.

Sabia que podia escrever algo que mostrasse a estudantes, desenvolvedores, consultores, engenheiros de segurança e outros o que era a criptografia aplicada moderna. Este seria um livro com poucas fórmulas, mas repleto de diagramas. Um livro com pouca história, mas cheio de histórias modernas sobre falhas criptográficas que eu testemunhei de verdade. Um livro com pouco sobre algoritmos legados, mas repleto de criptografia que eu pessoalmente vi sendo usada em larga escala: TLS, o framework de protocolo Noise, o protocolo Signal, criptomoedas, HSMs, criptografia com limiar e assim por diante. Um livro com pouca criptografia teórica, mas cheio do que pode vir a ser relevante: trocas de chaves autenticadas por senha, provas de conhecimento zero, criptografia pós-quântica, e por aí vai.

Quando a Manning Publications entrou em contato comigo em 2018, perguntando se eu queria escrever um livro sobre criptografia, eu já sabia a resposta. Eu já sabia o que queria escrever. Só estava esperando alguém me dar a

oportunidade e o pretexto para dedicar meu tempo escrevendo o livro que tinha em mente. Coincidentemente, a Manning tem uma série de livros "do mundo real", então naturalmente sugeri que meu livro a expandisse. O que você tem diante de si é o resultado de mais de dois anos de muito trabalho e muito amor. Espero que goste.

Agradecimentos

Obrigado a Marina Michaels por sua ajuda contínua e insights, sem os quais este livro provavelmente não teria sido concluído.

Obrigado a Frances Buran, Sam Zaydel, Michael Rosenberg, Pascal Knecht, Seth David Schoen, Eyal Ronen, Saralynn Chick, Robert Seacord, Eloi Manuel, Rob Wood, Hunter Monk, Jean-Christophe Forest, Liviu Bartha, Mattia Reggiani, Olivier Guerra, Andrey Labunov, Carl Littke, Yan Ivnitskiy, Keller Fuchs, Roman Zabicki, M K Saravanan, Sarah Zennou, Daniel Bourdrez, Jason Noll, Ilias Cherkaoui, Felipe De Lima, Raul Siles, Matteo Bocchi, John Woods, Kostas Chalkias, Yolan Romailler, Gerardo Di Giacomo, Gregory Nazario, Rob Stubbs, Ján Jančár, Gabe Pike, Kiran Tummala, Stephen Singam, Jeremy O'Donoghue, Jeremy Boone, Thomas Duboucher, Charles Guillemet, Ryan Sleevi, Lionel Rivière, Benjamin Larsen, Gabriel Giono, Daan Sprenkels, Andreas Krogen, Vadim Lyubashevsky, Samuel Neves, Steven (Dongze) Yue, Tony Patti, Graham Steel, e a todos os comentaristas do livebook pelas muitas discussões e correções, bem como feedbacks técnicos e editoriais.

A todos os revisores: Adhir Ramjiawan, Al Pezewski, Al Rahimi, Alessandro Campeis, Bobby Lin, Chad Davis, David T Kerns, Domingo Salazar, Eddy Vluggen, Gábor László Hajba, Geert Van Laethem, Grzegorz Bernaś, Harald Kuhn, Hugo Durana, Jan Pieter Herweijer, Jeff Smith, Jim Karabatsos, Joel Kotarski, John Paraskevopoulos, Matt Van Winkle, Michal Rutka, Paul Grebenc, Richard Lebel, Ruslan Shevchenko, Sanjeev Jaiswal, Shawn P Bolan, Thomas Doylend, William Rudenmalm — suas sugestões ajudaram a tornar este um livro melhor.

Sobre este livro

Já se passaram mais de dois anos desde que comecei a escrever *Real-World Cryptography*. Eu originalmente pretendia que fosse uma introdução a tudo o que há para saber sobre o tipo de criptografia que é usada no mundo real. Mas, é claro, essa é uma tarefa impossível. Nenhuma área pode ser resumida em um único livro. Por esse motivo, tive que encontrar um equilíbrio entre a quantidade de detalhes que eu queria oferecer ao leitor e a quantidade de tópicos que eu queria cobrir. Espero que você se encontre na mesma "caixa" em que eu acabei me colocando. Se você está procurando um livro prático que ensine a criptografia que empresas e produtos implementam e usam, e se você é curioso sobre como a criptografia do mundo real funciona por baixo dos panos, mas não está procurando um livro de referência com todos os detalhes de implementação, então este livro é para você.

Quem deve ler este livro

Aqui está uma lista do que acredito serem os tipos de pessoas (embora por favor, não deixe ninguém colocá-lo em uma caixa) que se beneficiariam deste livro.

Estudantes

Se você está estudando ciência da computação, segurança ou criptografia e quer aprender sobre a criptografia tal como é usada no mundo real (porque está mirando um emprego na indústria ou deseja trabalhar em assuntos aplicados na academia), então acredito que este seja o livro-texto para você. Por quê? Porque, como disse no prefácio, eu já fui um desses estudantes, e escrevi o livro que gostaria de ter tido então.

Profissionais de segurança

Pentesters, consultores de segurança, engenheiros de segurança, arquitetos de segurança e outros papéis relacionados compuseram a maioria dos alunos que tive quando lecionei criptografia aplicada. Por causa disso, este

material foi refinado pelas muitas perguntas que recebi enquanto tentava explicar conceitos criptográficos complicados para não-criptógrafos. Como eu também sou um profissional de segurança, este livro também é moldado pela criptografia que auditei para grandes empresas e pelos bugs que aprendi ou descobri ao longo do caminho.

Desenvolvedores que usam criptografia direta ou indiretamente

Este trabalho também foi moldado pelas muitas conversas que tive com clientes e colegas de trabalho, que em sua maioria não eram profissionais de segurança nem criptógrafos. Hoje em dia, está se tornando cada vez mais difícil escrever código sem tocar em criptografia e, como tal, você precisa ter algum entendimento do que está usando. Este livro fornece esse entendimento, com exemplos de código em diferentes linguagens de programação — e mais, se você for curioso.

Criptógrafos curiosos sobre outras áreas

Este livro é uma introdução à criptografia aplicada que é útil para pessoas como eu. Eu escrevi isso, primeiro, para mim mesmo, lembre-se. Se eu conseguir fazer um bom trabalho, um criptógrafo teórico deve ser capaz de obter rapidamente uma compreensão de como é o mundo da criptografia aplicada; outro, que trabalha com criptografia simétrica, deve conseguir entender rapidamente trocas de chaves autenticadas por senha lendo o capítulo correspondente; um terceiro, que trabalha com protocolos, deve conseguir adquirir rapidamente uma boa compreensão de criptografia quântica — e assim por diante.

Gerentes de engenharia e produto que querem entender mais

Este livro também tenta responder a perguntas que considero mais orientadas a produto: quais são as concessões e limitações dessas abordagens? Que risco estou assumindo? Este caminho me ajudaria a cumprir regulações? Preciso fazer isso e aquilo para trabalhar com um governo?

Pessoas curiosas que querem saber do que se trata a criptografia do mundo real

Você não precisa ser nenhum dos tipos listados anteriormente para ler este livro. Você só precisa ser curioso sobre a criptografia como usada no mundo real. Tenha em mente que eu não ensino a história da criptografia, e não ensino o básico da ciência da computação, então, no mínimo, você deveria ter ouvido falar de criptografia antes de começar um livro como este.

Conhecimento prévio presumido — a versão longa

O que você vai precisar para tirar o máximo proveito deste livro? Você deve saber que este livro assume que você tem algum entendimento básico de como seu laptop ou a internet funciona, e, pelo menos, deveria já ter ouvido falar de criptografia. O livro trata de criptografia do mundo real, e por isso será difícil colocar as coisas em contexto se você não se sentir à vontade com computadores ou se nunca ouviu a palavra “criptografia” antes.

Assumindo que você sabe mais ou menos no que está se metendo, será uma vantagem se você souber o que são bits e bytes, e se já viu ou até usou operações bit a bit como XOR, deslocamento à esquerda, e essas coisas. Isso é essencial? Não. Mas pode significar que você terá que parar de vez em quando para fazer algumas buscas antes de continuar a leitura.

Na verdade, não importa o quão qualificado você seja, ao ler este livro, provavelmente vai ter que parar de tempos em tempos para buscar mais informações na internet. Seja porque eu (vergonha!) esqueci de definir um termo antes de usá-lo, ou porque presumi erroneamente que você o conhecia. De todo modo, isso não deve ser um grande problema, pois tento explicar como se você tivesse 5 anos (EL5) da melhor forma possível os diferentes conceitos que introduzo.

Por fim, quando uso a palavra "criptografia", provavelmente você pensa em matemática. Se, além disso, você fez uma careta, então ficará feliz em saber que não precisa se preocupar tanto com isso. *Real-World Cryptography* trata de ensinar percepções para que você ganhe uma intuição sobre como tudo funciona, e tenta evitar ao máximo as minúcias matemáticas.

Claro, eu estaria mentindo se dissesse que não há matemática envolvida na produção deste livro. Não há como ensinar criptografia sem matemática. Então, aqui está o que eu direi: ajuda se você tem um bom nível de matemática, mas se não tem, isso não deve impedi-lo de ler a maior parte deste livro. Alguns capítulos serão menos amigáveis se você não tiver uma compreensão mais avançada de matemática — especificamente os capítulos finais (14 e 15) sobre criptografia quântica e de próxima geração —, mas nada é impossível, e você pode passar por esses capítulos com força de vontade e pesquisando sobre multiplicações de matrizes e outras coisas que talvez não conheça. Se decidir pular esses, certifique-se de não pular o capítulo 16, pois ele é a cereja do bolo.

Como este livro está organizado: Um roteiro

Real-World Cryptography está dividido em duas partes. A primeira parte deve ser lida da primeira à última página e cobre a maioria dos ingredientes da criptografia: as coisas que você acabará usando como peças de Lego para construir sistemas e protocolos mais complexos.

- **Capítulo 1** é uma introdução à criptografia do mundo real, dando uma ideia do que você irá aprender.
- **Capítulo 2** fala sobre funções de hash, um algoritmo fundamental da criptografia usado para criar identificadores únicos a partir de sequências de bytes.
- **Capítulo 3** fala sobre autenticação de dados e como você pode garantir que ninguém modifique suas mensagens.
- **Capítulo 4** fala sobre criptografia, que permite a dois participantes ocultarem suas comunicações de observadores.
- **Capítulo 5** introduz as trocas de chaves, que permitem negociar um segredo comum com outra pessoa de forma interativa.
- **Capítulo 6** descreve a criptografia assimétrica, que permite que várias pessoas criptografem mensagens para uma única pessoa.
- **Capítulo 7** fala sobre assinaturas, os equivalentes criptográficos das assinaturas feitas à caneta.
- **Capítulo 8** fala sobre aleatoriedade e como gerenciar seus segredos.

A segunda parte deste livro contém os sistemas que são construídos a partir desses ingredientes.

- **Capítulo 9** ensina como criptografia e autenticação são usadas para proteger conexões entre máquinas (via o protocolo SSL/TLS).
- **Capítulo 10** descreve a criptografia de ponta a ponta, que trata de como pessoas como você e eu podem confiar umas nas outras.
- **Capítulo 11** mostra como máquinas autenticam pessoas e como as pessoas podem ajudar as máquinas a se sincronizarem umas com as outras.
- **Capítulo 12** introduz o campo nascente das criptomoedas.
- **Capítulo 13** destaca a criptografia em hardware, os dispositivos que você pode usar para evitar que suas chaves sejam extraídas.

Há dois capítulos bônus:

- o **capítulo 14** sobre criptografia pós-quântica, e
- o **capítulo 15** sobre criptografia de próxima geração.

Esses dois campos estão começando a entrar em produtos e empresas, seja porque estão se tornando mais relevantes ou porque estão ficando mais práticos e eficientes.

Embora eu não vá julgá-lo se você pular esses dois últimos capítulos, você **tem** que ler o **capítulo 16** (palavras finais) antes de colocar este livro de volta na estante. O capítulo 16 resume os diferentes desafios e lições que um praticante de criptografia (ou seja, você, depois de terminar este livro) deve ter em mente. Como disse o Tio Ben do Homem-Aranha:
"Com grandes poderes vêm grandes responsabilidades."

Sobre o código

Este livro contém muitos exemplos de código-fonte, tanto em trechos numerados quanto incorporados ao texto comum. Em ambos os casos, o código-fonte é formatado com uma fonte de largura fixa, como esta, para separá-lo do texto comum. Às vezes, o código também aparece em **negrito** para destacar trechos que mudaram em relação a etapas anteriores no capítulo, como quando uma nova funcionalidade é adicionada a uma linha de código existente.

Em muitos casos, o código-fonte original foi reformatado; adicionamos quebras de linha e reorganizamos a indentação para acomodar o espaço disponível na página do livro. Em raros casos, mesmo isso não foi suficiente, e os trechos de código incluem marcadores de continuação de linha (➥). Além disso, comentários no código-fonte frequentemente foram removidos das listagens quando o código é descrito no texto. Anotações ao código acompanham muitas das listagens, destacando conceitos importantes.

Fórum de discussão do liveBook

A compra de *Real-World Cryptography* inclui acesso gratuito a um fórum web privado operado pela Manning Publications, onde você pode fazer comentários sobre o livro, fazer perguntas técnicas e receber ajuda do autor e de outros usuários. Para acessar o fórum, vá para:

https://livebook.manning.com/book/real-world-cryptography/discussion

Você também pode saber mais sobre os fóruns da Manning e sobre as regras de conduta em:

https://livebook.manning.com/discussion

O compromisso da Manning com seus leitores é fornecer um espaço onde um diálogo significativo entre leitores e entre leitores e o autor possa ocorrer. Isso **não é** um compromisso de participação específica por parte do autor, cuja contribuição ao fórum permanece voluntária (e não remunerada).

Sugerimos que você tente fazer ao autor algumas perguntas desafiadoras para que o interesse dele não se desvie!

O fórum e os arquivos de discussões anteriores estarão acessíveis no site da editora enquanto o livro estiver em catálogo.

Sobre o autor

DAVID WONG é engenheiro sênior de criptografia na **O(1) Labs**, trabalhando na criptomoeda **Mina**. Antes disso, ele foi o responsável pela segurança da criptomoeda **Diem** (anteriormente conhecida como **Libra**), na **Novi**, do Facebook. E antes disso, foi consultor de segurança na divisão de Serviços de Criptografia da **NCC Group**. David também é o autor deste livro, *Real-World Cryptography*.

Durante sua carreira, David participou de diversas auditorias de código aberto financiadas com recursos públicos, como **OpenSSL** e **Let's Encrypt**. Ele palestrou em várias conferências, incluindo **Black Hat** e **DEF CON**, e ministrou um curso recorrente de criptografia na Black Hat. Ele contribuiu para padrões como o **TLS 1.3** e o **Noise Protocol Framework**.

Ele encontrou vulnerabilidades em muitos sistemas, incluindo:

- CVE-2016-3959 (na biblioteca padrão do **Golang**),

- CVE-2018-12404,
- CVE-2018-19608,
- CVE-2018-16868,
- CVE-2018-16869, e
- CVE-2018-16870 (em várias bibliotecas TLS).

Entre outros feitos, ele é o autor do protocolo **Disco**:

- www.discocrypto.com
- www.embeddeddisco.com

e do projeto **DASP** (Decentralized Application Security Project) para contratos inteligentes:

- www.dasp.co

Sua pesquisa inclui:

- ataques de cache contra RSA: http://cat.eyalro.net/
- protocolos baseados em QUIC: https://eprint.iacr.org/2019/028
- ataques temporais contra ECDSA: https://eprint.iacr.org/2015/839
- backdoors em Diffie-Hellman: https://eprint.iacr.org/2016/644

Você pode vê-lo e ler sobre ele atualmente em seu blog:
www.cryptologie.net

Sobre a ilustração da capa

A figura na capa de *Real-World Cryptography* é legendada como **"Indienne de Quito"**, ou **Indiana de Quito**. A ilustração foi retirada de uma coleção de trajes de vestuário de diversos países feita por **Jacques Grasset de Saint-Sauveur (1757–1810)**, intitulada *Costumes de Diferents Pays*, publicada na França em 1797. Cada ilustração é finamente desenhada e colorida à mão.

A rica variedade da coleção de Grasset de Saint-Sauveur nos lembra vividamente o quão culturalmente distintas eram as cidades e regiões do mundo há apenas 200 anos. Isoladas umas das outras, as pessoas falavam dialetos e línguas diferentes. Nas ruas ou no campo, era fácil identificar onde elas viviam e qual era seu ofício ou posição na vida apenas observando suas vestimentas.

A maneira como nos vestimos mudou desde então, e a diversidade por região — tão rica naquela época — se dissipou. Agora é difícil distinguir os habitantes de diferentes continentes, muito menos de diferentes cidades, regiões ou países. Talvez tenhamos trocado diversidade cultural por uma vida pessoal mais variada — certamente por uma vida tecnológica mais variada e acelerada.

Em uma época em que é difícil distinguir um livro de informática de outro, a Manning celebra a inventividade e a iniciativa do setor de computação com capas de livros baseadas na rica diversidade da vida regional de dois séculos atrás, trazida de volta à vida pelas ilustrações de Grasset de Saint-Sauveur.